Duquesne Law Review

Volume 59 | Number 2 Article 8

2021

Too Big to Protect: A Dodd-Frank Framework for Protecting 21st Century American Consumer Privacy Rights

Stanley A. Marciniak III

Too Big to Protect: A Dodd-Frank Framework for Protecting 21st Century American Consumer Privacy Rights

Stanley A. Marciniak III[*]

* J.D. Candidate, Duquesne University School of Law, 2021; B.S.B.A., Robert Morris University, 2018. The author extends his heartfelt thanks to Professor Agnieszka McPeak for providing her invaluable suggestions and guidance, as well as to Professor John Rago for inspiring his passion for protecting privacy.

INTRODUCTION

In seemingly every area of one's daily economic interactions, consumers are protected by comprehensive legal frameworks—the Food and Drug Administration (FDA) ensures safe food and drugs are available in grocery stores, the National Highway Traffic Safety Administration (NHTSA) ensures cars have safe designs, the Federal Aviation Administration (FAA) ensures safe airline travel, and the Occupational Safety and Health Administration (OSHA) safeguards workplace conditions.[1] However, when consumers download an app, make an online purchase, or sign-up for a new digital service, it becomes difficult to point to a single comprehensive legal framework that protects consumer privacy in the United States. That is the focus of this article. American privacy law desperately needs wholesale reform to serve the needs of the twenty-first century consumer.

Part I of this article discusses the nature of the present consumer privacy crisis in American industry, examining recent data breaches, the privacy void consumers face, and the current lack of sufficient regulatory enforcement mechanisms.[2] Part II briefly explores the 2008 financial collapse, the origins of which contain numerous parallels to the present privacy crisis.[3] It primarily discusses the reform efforts following the financial crisis—namely the Dodd-Frank Act. Part III analogizes the 2008 financial crisis to the 2020 privacy crisis, highlighting the "Wild West" regulatory environment leading to each crisis, the development of economic bubbles, and tenuous corporate practices.[4] Finally, Part IV proposes a Dodd-Frank approach to comprehensive American consumer privacy legislation to respond to the current privacy crisis—articulating a "Data Fiduciary Rule," the creation of a Consumer Data Protection Bureau, and the promulgation of a Volcker rule for corporate data practices.[5]

---

1. WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 89 (2018).
2. *See infra* Part I.
3. *See infra* Part II.
4. *See infra* Part III.
5. *See infra* Part IV.

I. BACKGROUND: PRIVATE INDUSTRY'S PRIVACY CRISIS

In an interview with ABC News, Apple CEO Tim Cook stated that privacy in itself "has become a crisis."[6] The American public broadly shares Cook's sentiment. According to a March 2019 Axios poll, fifty-eight percent of American consumers believe the threat to online privacy is a crisis.[7] In the interview, Cook discussed the expansive amount of personal information available online, noting that "[t]he people who track on the internet know a lot more about you than if somebody's looking in your window . . . ."[8] Though privacy is a crisis, Cook believes it is a crisis that can be addressed—suggesting it is a problem solvable by united action.[9]

In 2013, the Organization for Economic Cooperation and Development (OECD) estimated that in developed nations, an average family of four had ten internet-connected devices in their home.[10] It is not hard to imagine, in the near future, devices that will produce data concerning one's diet, if they are home, and even whether they are having intimate relations.[11] This prospect becomes all the more disturbing when it is likely that these devices will be sharing information with corporate third-party entities. The number of internet-enabled devices—not just tablets and phones, but also things like smart refrigerators—has grown from 12.5 billion to 26.7 billion over the past decade.[12] Ben Zhao, a professor of computer science at the University of Chicago who studies security, privacy, and artificial intelligence,[13] notes that the firms manufacturing smart devices are often so small that "'there is no hope of ensuring that they're responsive' to privacy concerns . . . ."[14] There is no pressure for such firms to protect privacy as they have no public reputation, like industry giants such as Facebook.[15] More firms are now collecting, and possibly losing or abusing, individuals' data than ever

---

6. Lisa Eadicicco, *Apple CEO Tim Cook Says Digital Privacy 'Has Become a Crisis*,' BUS. INSIDER (May 4, 2019, 6:03 PM), https://www.businessinsider.com/apple-ceo-tim-cook-privacy-crisis-2019-5.

7. Kim Hart, *A Growing Majority Now Views Our Online Privacy as a Crisis*, AXIOS (Mar. 9, 2019), https://www.axios.com/a-growing-majority-now-views-our-online-privacy-as-a-crisis-1552080369-94146f05-332d-465d-a136-4414f9cdf9ce.html4.

8. Eadicicco, *supra* note 6.

9. *Id.*

10. HARTZOG, *supra* note 1, at 261.

11. *Id.* at 263–64.

12. Susie Allen, *The New Panopticon: Worried About Online Privacy? Computer Science Experts Worry Too*, U. OF CHI. MAG., Spring 2019, at 12.

13. *Id.*

14. *Id.*

15. *Id.*

before.[16] As an example of how ubiquitous the issue of data mining has become:

> [i]magine a seemingly innocuous retail app asking for permission to access your phone's built-in microphone. Without thinking much about it, you hit "allow." The simple tap of a button allows the app to listen for inaudible, high-pitched beacons emitted from its partner websites in addition to advertisements and storefronts. That means the company can know where you've been and what ads you've seen, online and offline.[17]

In short, "the company that makes your toaster knows you're a lefty who drives a Honda."[18] The fact that a growing number of the objects surrounding us are becoming internet-connected is a "prominent concern" for privacy.[19] More internet devices create a greater potential for data leaks, surveillance, and security vulnerabilities.[20]

Many regard privacy as a human right.[21] In many countries, the right to privacy is not explicitly protected, particularly on the internet.[22] Over the last three decades, there has been an aggressive erosion of privacy.[23] Most things on the internet appear to be "free."[24] But, they are not free. The public pays for them in other ways—via data and attention.[25] This is the price paid to Facebook for social networking and to Google for searches.[26] As individuals move throughout the world around them, they leave a trail of data behind them.[27] This electronic footprint left on the internet "tells a story."[28] The data generated by network-connected smart devices "is almost invariably sent to the cloud where it's carefully aggregated, packaged, and then usually sold."[29] The privacy and attention traded for the existence of "free" services and content is

16. *Id.*
17. *Id.*
18. *Id.*
19. HARTZOG, *supra* note 1, at 261.
20. *Id.*
21. Alasdair Allan, *The Coming Privacy Crisis on the Internet of Things*, MEDIUM (Oct. 8, 2017), https://medium.com/@aallan/has-the-death-of-privacy-been-greatly-exaggerated-f2c4f2423b5.
22. *Id.*
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. *Id.*

growing increasingly personal.[30] Now the data being shared, collected, and sold is not just "email[s] or the photographs of your cat, but your location, your heart rate, your respiration rate . . . [n]ot just how you slept last night, but with whom."[31] In short, connecting devices to the internet has resulted in poor privacy controls and poor security.[32] Consumers can avoid the death of privacy only if problems with smart devices continue to be "public relations nightmares for the companies involved."[33] "The loss of privacy may seem inevitable, but the only thing that makes it that way is our own apathy."[34]

Thus, "[t]here is no longer any question that data collection can create privacy harms for individuals: the question is what the law can and should do about it."[35] Currently, the central goal of American privacy law "is to create an environment where industry experiments first and asks questions later . . . ."[36] "Data collection by private entities is governed by a patchwork of state and federal law that applies on a sectoral basis."[37] If no sector-specific law applies, companies are free to collect data and use it at-will.[38]

But, if there is a privacy crisis, this raises the question of how exactly we define privacy. One way of defining privacy is "limited access to the self."[39] As it relates to privacy concerns in industry—primarily the overzealous collection, subsequent sale, and illicit use of personal information—this definition of privacy shall suffice for purposes of this article. After all, preventing exposure of one's personal information limits access to one's most intimate self. As an elaboration, privacy scholar Alan Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[40] The current landscape of privacy law in America, as well as globally, represents a "work in progress" held together by legal "duct tape" that "lacks cohesion."[41]

---

30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.*
34. *Id.*
35. Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1059 (2019).
36. *Id.* This is oddly reminiscent of KGB operatives during the Cold War, who shot first and asked questions later.
37. *Id.*
38. *Id.*
39. HARTZOG, *supra* note 1, at 10.
40. *Id.* at 63.
41. *Id.* at 56.

America's current "patchwork approach to privacy" allows some problems to go unnoticed and unsolved.[42] Exacerbating this issue, "lawmakers focus so intently on the details of complex, sector-specific statutes and regulations that they often fail to see the forest for the trees."[43] In short, America's legislators are not using all of their available tools to confront the privacy crisis.[44] Current disclosure-based regulatory regimes tend to "bury and obscure privacy-relevant information," overwhelming users.[45] One need only look at a single app's privacy policy to understand this. Consumers are most often confronted by:

> a threadbare, formalistic, or meaningless technical legal compliance . . . that overwhelms individuals with information and choices instead of substantively protecting them. It would be impracticable to read even a small fraction of the privacy notices we're asked to consent to or to forgo using the services we rely on . . . .[46]

If ordinary internet users were to read every single privacy policy they came across in the span of a year, it would take the user seventy-six working days to do so.[47] "[M]obile apps can seek over 235 . . . different types of permissions from smartphone users, with the average app asking for around five different permissions to access and use data."[48] Efforts to adapt the privacy torts to modern data collection and uses have failed.[49]

There is an inherent hypocrisy to the modern privacy crisis. "[W]hile powerful businesses, financial institutions, and government agencies hide their actions behind nondisclosure agreements . . . our own lives are increasingly open books. Everything we do online is recorded . . . ."[50] The decline in personal privacy has not been matched by business transparency. Credit agencies, search engines, and banks collect data about individuals, quantifying it into scores, rankings, and risk calculations while simultaneously shielding the details of the mechanisms by which they do so from

---

42. *Id.* at 57. For example, reliance on a web of statutes prevents privacy issues relating to overall technological design from being uniformly regulated.
43. *Id.*
44. *Id.*
45. *Id.* at 59.
46. *Id.* at 61.
47. *Id.* at 64.
48. *Id.* at 66.
49. *Id.* at 67.
50. FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 3 (2015).

public scrutiny.[51] Corporations "have unprecedented knowledge of the minutiae of our daily lives, while we know little to nothing about how they use this knowledge . . . ."[52]

As the internet has become ubiquitous, "personal data became substantially easier to access and track in ways unimaginable in decades prior."[53] Moreover, advanced algorithms allow utilization of personal data in a variety of fashions, "from predicting social trends to providing personalized financial advice."[54] Processing of personal data can yield social benefits while misuse of personal data can inflict personal harm upon individuals.[55]

A. Recent Data Breaches & the Privacy Void

Recent consumer data breaches provide a helpful illustration of the privacy crisis described above.

1. The Equifax Data Breach

In September 2017, Equifax, one of the three largest consumer credit reporting agencies in the United States, announced that its systems had been compromised.[56] The data breach included "names, home addresses, phone numbers, dates of birth, social security numbers, and driver's license numbers. The credit card numbers of approximately 209,000 consumers were also breached."[57] Federal Trade Commission (FTC) Chairman Joe Simons asserted that Equifax "failed to take basic steps that may have prevented the breach that affected approximately 147 million consumers."[58] The FTC claimed "Equifax failed to patch its network after being alerted in March 2017 to a critical security vulnerability . . . ."[59] Hackers were able to access a staggering amount of data because Equifax failed to implement basic security concerns.[60] The FTC also claimed Equifax stored network credentials and passwords, as well

51. *Id.* at 4.
52. *Id.* at 9.
53. Tyler Stites, *Data Protection on the Doorstep: How the GDPR Impacts American Financial Institutions*, 38 REV. BANKING & FIN. L. 132, 132 (2018).
54. *Id.*
55. *Id.*
56. *Equifax Data Breach*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/data-breach/equifax/ (last visited Sept. 22, 2019).
57. *Id.*
58. Press Release, Fed. Trade Comm'n, Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [hereinafter FTC Press Release].
59. *Id.*
60. *Id.*

as Social Security numbers and other sensitive consumer information, in plain text.[61] Ironically, "[d]espite its failure to implement basic security measures, Equifax's privacy policy at the time stated that it limited access to consumers' personal information and implemented 'reasonable physical, technical, and procedural safeguards' to protect consumer data."[62] Unfortunately, Equifax's response to the data breach was not entirely successful. Its response to the breach "raised concerns among security experts and consumer advocates," with security expert Brian Krebs labeling Equifax's response to the breach as a "dumpster fire."[63] Moreover, consumers who contacted Equifax following the breach to freeze their credit were given PINs that corresponded to the date and time of the freeze, making the PINs easier for criminals to guess.[64]

Both the FTC and Consumer Financial Protection Bureau (CFPB) investigated the Equifax Data Breach.[65] As a result of the data breach, Equifax agreed to pay at least $575 million, and potentially up to $700 million, as part of a global settlement with the FTC, CFPB, and fifty states and territories.[66] After a settlement with Equifax, affected consumers could file a claim for free credit monitoring or accept a cash payment of $125.[67] Moreover, "beginning in January 2020, Equifax will provide all U.S. consumers with six free credit reports each year for seven years . . . ."[68] But, credit monitoring or a few dollars cannot truly compensate the loss of one's privacy, particularly with respect to sensitive information like social security numbers. However, Equifax even botched the management of its settlement. The public response to the settlement has been overwhelming.[69] Because the amount of money set aside for the cash payment option is capped at $31 million, consumers who select that option may not receive the $125 they expected.[70]

61. *Id.*
62. *Id.*
63. *Equifax Data Breach*, *supra* note 56.
64. *Id.*
65. *Id.*
66. *See* FTC Press Release, *supra* note 58.
67. *Equifax Data Breach*, *supra* note 56.
68. FTC Press Release, *supra* note 58.
69. Press Release, Fed. Trade Comm'n, FTC Encourages Consumers to Opt for Free Credit Monitoring, as Part of Equifax Settlement (July 31, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-encourages-consumers-opt-free-credit-monitoring-part-equifax.
70. *Id.*

2. The Capital One Data Breach

In July 2019, a Seattle software engineer hacked into a server holding Capital One's customer information, obtaining the personal data of over 100 million people.[71] The culprit stole 140,000 Social Security numbers and 80,000 bank account numbers in the breach, later boasting online a desire to "distribute" the information.[72] Capital One has suffered prior security breaches. In 2017, the same year as the Equifax breach, Capital One reported that a former employee had access to consumers' personal data for nearly four months, including account numbers, telephone numbers, transaction history, and Social Security numbers.[73] Security breaches are a continuous threat to the financial industry. JPMorgan Chase executive Jamie Dimon has stated that his company spends nearly $600 million per year on security.[74] Similarly, Bank of America has said that its budget for cybersecurity is a blank check.[75]

3. Other Significant Data Breaches

Organizations like Anthem, Blue Cross Blue Shield, T-Mobile, the Internal Revenue Service, and the United States Army National Guard have all experienced data breaches in recent years.[76] Yet, the privacy void we face is not the result of corporate "evil" or malintent. In fact, many business executives expressly state their concerns for the privacy of their consumers and user base;[77] rather, such issues are the result of "overwhelming" economic initiatives to "design technologies in a way that maximizes the collection, use, and disclosure of personal information."[78] Opponents of additional privacy regulations on industry claim that "[w]e already have effective privacy laws that prevent harmful collection, use, and disclosure of personal information . . . ."[79] However, "[a] study by the Pew Research Center found that most adults do not believe online service providers will keep their data private and secure."[80]

---

71. Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of over 100 Million*, N.Y. TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. HARTZOG, *supra* note 1, at 3.
77. *Id.* at 4.
78. *Id.* at 5.
79. *Id.*
80. *Id.* at 6.

There have been numerous data breaches in recent years. For example, a 2013 breach of Yahoo resulted in the theft of names, birth dates, phone numbers, and passwords impacting nearly three billion users of the site worldwide.[81] A 2015 breach of the federal government's Office of Personnel Management resulted in exposure of the personal data of more than twenty million people, including many with government security clearances.[82] Data breaches of Chipotle, Home Depot, and Target impacted over 100 million individuals, whose credit card numbers were stolen.[83]

Data breaches create considerable problems for consumers stemming from the loss of privacy. One such problem is identity theft.[84] The FTC reported 399,225 cases of identity theft in the United States in 2016.[85] Of that number, twenty-nine percent involved the use of personal data to commit tax fraud.[86] More than thirty-two percent reported that their data was used to commit credit card fraud.[87] Additionally, a 2015 report from the Department of Justice estimated the cost of identity theft to the American economy at $15.4 billion.[88] For an individual consumer, identity theft can result in denial of credit for credit cards and loans, denial of housing, increased interest rates on existing credit cards, and emotional distress and anxiety.[89]

Privacy is being eroded "click by click."[90] Those concerned with privacy most often ask how they can protect themselves in the age of data collection and data breach.[91] But, this begs the question: why must individuals protect themselves in the realm of privacy when the law shields the public for protective purposes in other facets of life, such as operating a motor vehicle, financial services, and criminal justice? This article argues that individuals should not have to.

B. The Lack of Federal Trade Commission Enforcement Power

Given the current state of privacy law in the United States, a private actor not falling under the definition of a narrowly defined,

81. *Equifax Data Breach*, *supra* note 56.
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. *Id.*
90. HARTZOG, *supra* note 1, at 6.
91. Allen, *supra* note 12, at 12.

sector-specific privacy statute "can largely do whatever it wants with the data it collects or otherwise obtains, provided it does not lie about its actions and attract the attention of an overstretched FTC."[92] Presently, the FTC is the primary federal agency tasked with protecting individuals from privacy exploitation from commercial entities as it pertains to data privacy, data security, and data misuse.[93]

The FTC asserts that "[w]hen companies tell consumers they will safeguard their personal information," it takes legal action to ensure companies fulfill their promises.[94] One of the only major federal legal frameworks in the United States addressing privacy in the consumer realm is Section 5 of the Federal Trade Commission Act.[95] In many instances of consumer privacy issues, the FTC charges corporations with violation of Section 5 of the FTC Act.[96] Specifically, Section 5(a) of the FTC Act declares unlawful "[u]nfair or deceptive acts or practices in or affecting commerce . . . ."[97]

However, there are substantial limits to the FTC's ability to protect consumer privacy. Any company within the FTC's jurisdiction that uses consumer information in a way that constitutes an unfair or deceptive trade practice is subject to the FTC's oversight.[98] The FTC is essentially the "sole backstop for the weaknesses of the rest of U.S. consumer privacy law . . . ."[99] In short, the FTC can only do so much. Moreover, the FTC's authority does not include common carriers or non-profits.[100] The FTC also lacks the general rulemaking authority of other administrative agencies, policing industry only on a reactive, case-by-case basis.[101] In privacy and data security cases, the FTC typically only utilizes its "deception" authority and rarely relies on its "unfairness" authority.[102] This means that the FTC's monitoring of privacy abuses remains limited to those instances when a company is not forthright about its practices, "regardless of whether the practice itself is inherently abusive . . . ."[103] Because most privacy policies are "difficult to understand" and

92. Barrett, *supra* note 35, at 1061–62.
93. *Id.* at 1073.
94. *Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Sept. 22, 2019).
95. *See generally* 15 U.S.C.A. § 45.
96. *Privacy and Security Enforcement*, *supra* note 94.
97. 15 U.S.C.A. § 45(a)(1).
98. Barrett, *supra* note 35, at 1073–74.
99. *Id.* at 1074.
100. *Id.*
101. *Id.*
102. *Id.* at 1075.
103. *Id.*

"rarely read," the FTC's reliance on deception-based enforcement is relatively narrow, allowing corporations to escape legal scrutiny so long as their privacy policies remain truthful, even if exploitative.[104] The FTC's regulatory approach follows no more than an insufficient "do not lie" approach to privacy.[105]

As data breaches become more pervasive and devastating, the FTC is becoming increasingly reluctant to comment on even egregious cases of consumer privacy infractions.[106] The FTC lacks the economic teeth necessary to realistically punish corporations for privacy transgressions. The FTC's powers do not have a "serious deterrent effect" for preventing mishandling of our private information.[107] The largest privacy fine the FTC ever imposed is $5 billion.[108] For comparison, Facebook's 2018 revenue alone was approximately $56 billion, "making the likelihood of a fine that will meaningfully change the company's approach decidedly slim."[109] Overall, the FTC's privacy enforcement mechanisms are "deliberately laissez-faire."[110] This is a fundamental shortcoming because "protecting consumers in a twenty-first century economy where ubiquitous commercial surveillance can both harm consumers and have anticompetitive effects requires an FTC that can *prevent* new kinds of informational harms, not simply *react* to them."[111] As it stands, the nation's largest companies lack a sufficient check on abusive, privacy-invasive practices.[112] In fact, "[t]here is little in current law to prevent companies from selling their profiles of you."[113]

II. THE ADOPTION OF THE DODD-FRANK ACT

The 2008 economic collapse, known as the Great Recession,[114] would be among the worst in American history, rivaling only the

104. *Id.*
105. HARTZOG, *supra* note 1, at 67–68.
106. Barrett, *supra* note 35, at 1075–76; *see, e.g.*, Taylor Telford & Craig Timberg, *Marriott Discloses Massive Data Breach Affecting up to 500 Million Guests*, WASH. POST (Nov. 30, 2018, 1:03 PM), https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/.
107. PASQUALE, *supra* note 50, at 23.
108. Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making*, FED. TRADE COMM'N (July 24, 2019, 8:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.
109. Barrett, *supra* note 35, at 1076–77.
110. *Id.* at 1077.
111. *Id.* (emphasis added).
112. *Id.*
113. PASQUALE, *supra* note 50, at 32.
114. For a comprehensive overview of the causes and consequences of the 2008 financial crisis, *see* FREDERIC S. MISHKIN, THE ECONOMICS OF MONEY, BANKING, AND FINANCIAL

Great Depression. The Great Recession led to economic despair that was unprecedented in twenty-first century America. Economic growth declined for three straight quarters in late 2008 and early 2009, by 1.3%, 5.4%, and 6.4% respectively.[115] Unemployment rose to over ten percent in the United States.[116]

The Great Recession led to the adoption of several regulatory regimes that changed the landscape of how government entities approached economic regulation in the financial sector. Following the collapse, the government's regulatory focus shifted from monitoring the economic soundness of "individual" financial institutions to the health of the financial "system."[117] One major reform was the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank).[118] Dodd-Frank "is the most comprehensive financial reform legislation since the Great Depression."[119] Its key provisions include consumer protection provisions, resolution authority for oversight entities, systemic risk regulation, the Volcker Rule, and regulation of derivatives.[120]

A. The Consumer Financial Protection Bureau

One of the major provisions of Dodd-Frank was the creation of the Consumer Financial Protection Bureau (CFPB), a "completely independent"[121] agency tasked with examining and enforcing regulations on all businesses with more than $10 billion in assets engaged in issuing residential mortgage products as well as on issuers of financial products targeted at low-income Americans.[122] "For consumer financial services, the centerpiece of the Dodd-Frank Act was the creation of the [CFPB]."[123] Congress vested the CFPB with the consumer financial protection functions of numerous federal agencies and gave the CFPB broad authority over segments of the consumer financial services market not previously subject to federal

---

MARKETS 274–86 (4th ed. 2015). The modern privacy landscape suffers from similar technological and information-based issues that led to the collapse. *See generally* PASQUALE, *supra* note 50, at 4–5. However, the focus of this article is how parallel *reform* efforts can address these parallel *issues*.

115. MISHKIN, *supra* note 114, at 282.
116. *Id.*
117. *Id.* at 283–84.
118. *Id.* at 284; *see also* 12 U.S.C.A. §§ 5301–5641.
119. MISHKIN, *supra* note 114, at 284.
120. *Id.* at 284–85.
121. *Id.* at 284.
122. *Id.*
123. Donald C. Lampe & Ryan J. Richardson, *The Consumer Financial Protection Bureau at Five: A Survey of the Bureau's Activities*, 21 N.C. BANKING INST. 85, 85 (2017).

regulation.[124] The CFPB serves three primary functions: rulemaking, supervision, and enforcement.[125]

Like the Consumer Data Protection Bureau called for later in this article,[126] the CFPB's origins lie in legal academia, as "calls to consolidate federal consumer financial protection functions in a single federal agency predated the financial crisis."[127] In 2005, Professor Heidi Mandanis Schooner of Catholic University argued that banking regulatory agencies' consumer protection responsibilities should be assigned to a single consumer protection agency.[128] In 2007, then-Professor Elizabeth Warren of Harvard University argued in an article entitled "Unsafe at Any Rate" that "streamlined federal consumer protections in the market for tangible goods (like toasters) had successfully balanced the twin goals of protecting consumers and promoting innovation."[129] In contrast, a fragmented regulatory framework in the financial services market had done the exact opposite, failing to protect consumers and limiting innovation.[130] Warren suggested the creation of a Financial Product Safety Commission to create guidelines for consumer disclosure, collect data regarding the uses of financial products, review financial products for consumer safety, and require modification of certain dangerous products before they could be marketed to the public.[131]

Dodd-Frank provides the CFPB with broad rulemaking, supervisory, and enforcement power over the consumer financial services market.[132] Congress gives the CFPB authority over "covered persons," which includes "'any person that engages in offering or providing a consumer financial product or service' and 'any affiliate of [such a person if the] affiliate acts as a service provider to the covered person.'"[133] Under Dodd-Frank, the CFPB can require reports and examinations of "covered persons" and "service providers" to assess their compliance with the law by obtaining information about their activities and compliance systems while detecting risks

124. *Id.*
125. *Id.* at 86.
126. *See infra* Part IV.B.
127. Lampe & Richardson, *supra* note 123, at 90.
128. *Id.* at 91. *See generally* Heidi Mandanis Schooner, *Consuming Debt: Structuring the Federal Response to Abuses in Consumer Credit*, 18 LOY. CONSUMER L. REV. 43, 67–77 (2005).
129. Lampe & Richardson, *supra* note 123, at 91. *See generally* Elizabeth Warren, *Unsafe at Any Rate*, DEMOCRACY J., http://democracyjournal.org/magazine/5/unsafe-at-any-rate/ (last visited Sept. 8, 2020).
130. Lampe & Richardson, *supra* note 123, at 91.
131. *Id.*
132. *Id.* at 97.
133. *Id.* at 95.

to consumers and markets in the realm of consumer financial products and services.[134]

The CFPB also has the power to "enforce" federal consumer financial law, including Title X of Dodd-Frank and rules created under Title X.[135] Dodd-Frank provides the CFPB with three primary enforcement tools: (1) investigation of potential violations of federal consumer financial law; (2) the ability to bring public legal actions in federal court or an administrative forum for violations of federal consumer financial law; and (3) the ability to seek injunctive and monetary relief for violations of federal consumer financial law.[136] The CFPB may demand document production, written responses, and oral testimony if it "has reason to believe that any person may be in possession, custody, or control of any documentary material or tangible things, or may have any information" relevant to a violation of consumer financial law.[137] While the CFPB's rulemaking and supervisory authorities only apply to "covered persons," its broad enforcement authority applies to any "person," resulting in a "sweeping, plenary power."[138]

The CFPB is flexible in its approach, adapting to necessary consumer protection issues as they arise via market developments. But, as much as the CFPB has earned praise from "members of Congress, consumer and community advocates and others," it has also "attracted the attention of policymakers intent on modifying the agency's structure and slimming down its powers," such as the Trump Administration.[139] The impact of the CFPB has been significant in its short history. It has "facilitated approximately $11.7 billion in consumer redress and $440 million in penalties . . . while promulgating thousands of pages of complex, wide-ranging regulations mandated or contemplated by the Dodd-Frank Act," while also conducting over 100 examinations.[140]

B. The Fiduciary Rule

One of Dodd-Frank's major reforms included the "Fiduciary Rule."[141] "The Fiduciary Rule requires financial advisers to act in the best interests of their clients regarding retirement planning

134. *Id.* at 104.
135. *Id.* at 106.
136. *Id.* at 107.
137. *Id.* at 108.
138. *Id.* at 107.
139. *Id.* at 128.
140. *Id.* at 127–28.
141. Corey F. Schechter, *Dodd-Frank and the Fiduciary Rule*, BUTTERFIELD SCHECHTER LLP (Mar. 21, 2017), https://www.bsllp.com/dodd-frank-and-the-fiduciary-rule.

. . . ."[142] The Fiduciary Rule was a package of seven different rules that re-interpreted the term "investment advice fiduciary" to encompass a wider variety of financial transactions.[143]

Beginning in 2010, the Department of Labor set out to overhaul the investment advice fiduciary definition.[144] Monumentally important to the financial services sector, the Fiduciary Rule consisted of 275 pages of regulations.[145] The Fiduciary Rule's definition of "investment advice fiduciary" encompassed "virtually all financial and insurance professionals who do business with ERISA plans and IRA holders."[146] The Fiduciary Rule also included a Best Interest Contract Exemption (BICE), allowing certain financial services providers to be exempt from the penalty provisions of the rule.[147] To qualify for an exemption, financial services providers would need to enter into contracts with clients that affirm their fiduciary status, incorporate impartial conduct standards including the duties of loyalty and prudence, avoiding misleading statements, and that "charge no more than 'reasonable compensation.'"[148]

However, despite its novelty, the reign of the fiduciary rule was short-lived, as its politically charged[149] nature led to its challenge in federal court by business groups.[150] In 2018, the Fifth Circuit vacated the rule,[151] "effectively put[ting] an end" to its operation.[152] Consumer advocates labeled the Fifth Circuit decision as "tragic," noting its implication that consumers would be "on their own" in looking out for their financial interests.[153] However, the Securities and Exchange Commission (SEC), whom Dodd-Frank specifically

142. *Id.*
143. Chamber of Com. v. U.S. Dep't of Lab., 885 F.3d 360, 363 (5th Cir. 2018).
144. *Id.* at 366.
145. *Id.*
146. *Id.*
147. *Id.* at 366–67.
148. *Id.* at 367.
149. *See* Schechter, *supra* note 141. The Fiduciary Rule received significant support from the Obama Administration as well as consumer advocates, hailing its ability to minimize investment advisers' potential conflicts of interest. *Id.* Alternatively, the Trump Administration and financial institutions viewed the rule as a burdensome mechanism that would hurt middle-class investors. *Id.*
150. *Chamber of Com.*, 885 F.3d at 363.
151. *Id.* at 387. In vacating the Fiduciary Rule, the Fifth Circuit characterized it as a backdoor regulation of a significant portion of the American economy. *Id.* at 388.
152. Lorie Konish, *Investor Protection Rule Is Dead*, CNBC (June 21, 2018, 3:30 PM), https://www.cnbc.com/2018/06/21/investor-protection-rule-is-dead.html.
153. *Id.*

authorized to create its fiduciary standard, has plans of proposing its own fiduciary standard.[154]

C. The Volcker Rule

One of Dodd-Frank's key risk management provisions is known as the Volcker Rule.[155] The Volcker Rule consists of a regulatory provision that limits the extent to which banks can trade with depositors' money.[156] This rule also prevents banks from owning more than just a small percentage of shadow entities such as hedge funds and private equity funds.[157] The rule prevents banks from undertaking large trading risks when they benefit from the safety net of federal deposit insurance.[158] As an analogy, the Volcker Rule of Dodd-Frank seeks to limit the moral hazard problem similar to that of a gambler using someone else's money: "I do not care if I lose $20,000 when my friend's money essentially insures me for $40,000." Thus, the Volcker Rule handcuffs banks from "gambling" their depositors' money.

III. ANALOGIZING THE CRISES: TOO BIG TO FAIL VS. TOO BIG TO PROTECT

In many ways, the modern privacy crisis resembles the 2008 financial crisis. In the sections below, these parallels are explored: the "Wild West" regulatory environment present in both realms, the data collection bubble currently arising in twenty-first century life (similar to the housing market bubble), and problems arising from the corporate use and sale of consumer data (similar to the frequent re-sale of mortgages by financial institutions prior to the financial crisis).

A. The "Wild West" Regulatory Environment

Specifically, the regulatory environment for American consumer privacy in 2019 largely parallels the pre-2008 Wall Street regulatory environment in terms of the weakness of the industry protections present in the current law. In the United States, "no comprehensive federal privacy or cybersecurity legislation has been

154. *Id.* The SEC would adopt a best-interest standard for investment advisers and broker dealers that make recommendations to retail investors, covering far more than just retirement accounts. *Id.*

155. MISHKIN, *supra* note 114, at 285.

156. *Id.*

157. *Id.*

158. *Id.*

enacted . . . ."[159] In recent years, there has been a "dramatic increase in devastating cyberattacks" and an increase in the "sophistication of hackers."[160] Even to businesses, "[c]yberattacks can be incredibly costly . . . as the company's data may be temporarily unavailable, destroyed, or even stolen or misused."[161] The 2019 consumer privacy landscape also resembles the Wild West, as "lax enforcement makes perfect sense in an environment where platforms want as many users as possible, as many app purchases as possible, and as many ad clicks as possible."[162] American privacy law "needs a radical course correction, not a mere adjustment."[163]

Corporations are not being entirely forthcoming with how they handle privacy. In 2014, Snapchat "ran afoul of the FTC for lying about how ephemeral its communications were."[164] The current concepts of notice and disclosure are also flawed. "[P]rivacy law still prioritizes technical compliance over meaningful disclosure when demanding notice."[165] Mortgage disclosures prior to 2008, as discussed above were similarly opaque. Woodrow Hartzog, a privacy scholar at Northeastern University School of Law, cautions, however, that "[p]rivate causes of action for privacy violations should be exceptions to the general rule of compliance."[166] Reform must target proactive solutions, rather than reactive panic.

In sum, "[m]ost data privacy laws within the U.S. are fragmented, regulating specific states or industries."[167] FTC regulatory authority derives mostly from enforcing company-issued privacy policies.[168] Dodd-Frank allowed the CFPB to study and regulate data portability in the United States.[169] Yet, the CFPB's current leadership takes a largely "inactive" approach to such regulation.[170] This essentially is a modified self-regulatory scheme, a potential recipe for disaster in the privacy realm. As Johnnie Cochran famously quipped in the O.J. Simpson trial, who is going to "police

159. Daniel Ilan et al., *Data Privacy and Cybersecurity in M&A: A New Era*, 10 LANDSLIDE 48, 50 (2018).
160. *Id.* at 49.
161. *Id.* at 50.
162. Barrett, *supra* note 35, at 1096.
163. *Id.* at 1113.
164. PASQUALE, *supra* note 50, at 123.
165. HARTZOG, *supra* note 1, at 69.
166. *Id.* at 83.
167. Stites, *supra* note 53, at 139.
168. *Id.*
169. *Id.* at 142.
170. *Id.*

the police?"[171] "[S]elf-regulation alone is not going to cut it" in terms of privacy protections in the twenty-first century.[172] Numerous incentives exist for companies to "design consumer technologies in ways that are adversarial" to our privacy interests.[173]

The time is ripe for reform. The business scandals of the late nineteenth century Gilded Age sparked bold legal reforms when the American public demanded business be held accountable to public scrutiny.[174] Such efforts intensified following the Great Depression in the form of the New Deal.[175] Numerous pieces of landmark legislation were passed to peel back the unnerving shroud of secrecy that encapsulated American industry and Wall Street.[176] America saw passage of the Securities Act of 1933 and the Securities and Exchange Act of 1934.[177] Throughout the twentieth century, a push for consumer protection led to the creation of new federal agencies, such as the FDA and the Consumer Product Safety Commission.[178] However, with the rise of the new millennium and the dawn of the age of Google, a cloak of corporate secrecy re-arose.[179] Internet technologies are spreading, "unmonitored and unregulated."[180]

B. The Data Collection Bubble

Privacy issues could be exacerbated if the economy's new "[t]ech [b]ubble" bursts.[181] Just about every company now holds user data.[182] If this data bubble bursts, what will be left of massive companies like Facebook and Twitter? Likely, "the only thing worth salvaging from the shells of former tech companies may be user data."[183] As for what the aftermath of a collapse would look like from a data perspective, consider the bankruptcy of RadioShack. When RadioShack filed for bankruptcy, "one of the assets it put up for sale was its meticulously compiled database of information on

171. David Margolick, *With Tale of Racism and Error, Simpson Lawyers Seek Acquittal*, N.Y. TIMES (Sept. 29, 1995), https://www.nytimes.com/1995/09/29/us/with-tale-of-racism-and-error-simpson-lawyers-seek-acquittal.html.
172. HARTZOG, *supra* note 1, at 72.
173. *Id.*
174. PASQUALE, *supra* note 50, at 11.
175. *Id.*
176. *Id.*
177. *Id.*
178. *Id.* at 12.
179. *Id.* at 13.
180. *Id.* at 14.
181. Kaveh Waddell, *Who Will Own Your Data If the Tech Bubble Bursts?*, THE ATLANTIC (May 13, 2016), https://www.theatlantic.com/technology/archive/2016/05/what-happens-to-your-data-if-the-tech-bubble-bursts/482622/.
182. *Id.*
183. *Id.*

millions of its customers."[184] Soon thereafter, AT&T and Apple claimed to own some of the data, and "officials in a handful of states warned that the sale could violate state laws."[185]

"Corporations, data brokers, and even criminals might buy failed companies just for their users' personal information."[186] Companies may resort to selling user data—"whether it's personally identifiable information, data about preferences, habits, and hobbies, or national-security files."[187] This data could be attractive to both business and criminal buyers.[188] "If contracts and privacy policies prevent a floundering company from selling user data, there's still another way to profit. Most privacy policies that promise not to sell user data include a caveat in case of bankruptcy or sale."[189] A New York Times analysis of 100 of the top web sites in the United States last year found that eighty-five percent of them include clauses in their privacy policies, providing that "[i]f the ownership or control of all or part of our [s]ervices or their assets change[], we may transfer your information to the new owner."[190] This type of transfer of data bears resemblance to the securitization and subsequent sale of packages of mortgage loans in 2008 by failing financial services organizations.[191] If the tech bubble bursts, it is unlikely that the FTC would have appropriate enforcement power to "keep up with the sheer number of previously overvalued data-rich companies offering themselves . . . for sale."[192] Without any other legal remedy in place, "the post-bubble technology industry will take your data down with it . . . ."[193]

IV. THE DODD-FRANK APPROACH FOR AMERICAN PRIVACY

If Americans cannot stop "pervasive" data collection, use, and sale, the question becomes: "[w]hat do we do?"[194] Self-help through privacy-enhancing technologies like "do not track" functions in internet browsers will likely fail "on practical grounds for all but the most skilled (or wealthy) Internet users . . . ."[195] Each day that

184. *Id.*
185. *Id.*
186. *Id.*
187. *Id.*
188. *Id.*
189. *Id.*
190. *Id.*
191. *See generally* MISHKIN, *supra* note 114, at 274–86.
192. Waddell, *supra* note 181.
193. *Id.*
194. PASQUALE, *supra* note 50, at 52.
195. *Id.* at 53–54.

privacy "enhancing" technology emerges, so does privacy "eviscerating" technology.[196] In short, the answer lies in the law. Imposing accountability-based legal structures on corporations that define "fair and unfair uses of information" can catalyze a solution.[197] This article proposes a Dodd-Frank approach to comprehensive American consumer privacy legislation based upon three prongs: (1) fiduciary responsibilities; (2) the creation of a Consumer Data Protection Bureau; and (3) the promulgation of a "Volcker Rule" for data privacy.

A. Mandate of Data Fiduciary Responsibilities

To be effective, comprehensive consumer privacy legislation should include a mandate of fiduciary responsibilities upon certain data-collecting American businesses who share a special relationship to consumers because of consumers' trust in these businesses with their most sensitive information. In short, businesses would be subject to fiduciary responsibilities when holding themselves out as organizations who give consumers reason to believe personal consumer data will not face unreasonable disclosure or misuse. Such an idea is not outlandish or even without legislative support. Senator Brian Schatz, as well as fourteen other Senators, have already proposed the Data Care Act, a comprehensive legislative framework that "sketches out broad duties of loyalty, care, and confidentiality, while providing the FTC with rulemaking authority to determine the details."[198]

Though market forces are often powerful in curbing illicit business behavior, here they are likely to be insufficient. A mandate is necessary because "a voluntary [information fiduciary regulatory] regime shaped by the lobbyists for the companies it would purport to regulate will be subject to the same broad provisions and tepid commitments of other self-regulatory programs that have been largely ineffective."[199] All else being equal, "companies like Facebook or Google would like to maximize the value of the personal data they collect" as "end-user data is one of [a company's] most valuable assets."[200] But, its status as a central component of many companies' business models "creates an inherent potential for

196. *Id.* at 53.
197. *Id.* at 57.
198. Barrett, *supra* note 35, at 1094.
199. *Id.* at 1093.
200. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1226 (2016).

conflicts of interest" between the company and the consumer.[201] Additionally, reliance upon market forces alone to solve these conflict of interest problems is insufficient.[202] Though the market *can* punish companies with bad reputations for mistreating their consumers, "there is no guarantee that this will be enough to effectively police all forms of misbehavior."[203] Personal data is a source of wealth in the digital economy.[204] Because of this, information fiduciaries "should be able to monetize some uses of personal data . . . ."[205] What they should not be able to do is "use the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm."[206]

1. The Jack Balkin "Information Fiduciaries" Concept

Privacy is not at odds with business development and innovation. As Professor Jack Balkin of Yale Law School recognizes, "personal privacy in the digital age can co-exist with rights to collect, analyze, and distribute information that are protected under the First Amendment . . . through the concept of an *information fiduciary*."[207] "[M]any online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should be seen as information fiduciaries toward their customers and end-users."[208] Modern consumer businesses rooted in digital technology possess special power and relationships with others. Accordingly, Balkin argues that information fiduciaries have "special duties to act in ways that do not harm the interests of the people whose information they collect, analyze, use, sell, and distribute."[209] However, as a responsible basis for a privacy regulatory framework, the duties information fiduciaries owe must be contextually related to both the nature of their business and the expectations of the public.[210]

This begs the question, however, of what a fiduciary is. A fiduciary is "one who has special obligations of loyalty and trustworthiness toward another person," taking care to act in the interests of

201. *Id.*
202. *Id.*
203. *Id.*
204. *Id.* at 1227.
205. *Id.*
206. *Id.*
207. *Id.* at 1186.
208. *Id.*
209. *Id.*
210. *Id.*

the other person—known as the beneficiary or client.[211] At its core, a fiduciary relationship is a relationship of trust.[212] A client puts their trust or confidence in the fiduciary, and the fiduciary must avoid betraying the client's confidence or trust.[213] Fiduciaries may perform professional services or manage property for a client,[214] but they do not necessarily have to. Yet, almost always, fiduciaries "also handle sensitive personal information" as fiduciary relationships "involve the use and exchange of information."[215] Modern consumer interactions are no different.

Generally, fiduciaries have two basic duties to their beneficiaries: a duty of care and a duty of loyalty.[216] First, the duty of care requires the fiduciary to "act competently and diligently so as not to harm the interests" of the beneficiary.[217] Second, the duty of loyalty requires the fiduciary to keep their beneficiaries' interests at heart and act in the beneficiaries' interests.[218] At the heart of these duties are relationships "often centrally concerned with the collection, analysis, use, and disclosure of information."[219] Therefore, a fiduciary also has a duty "not to use information . . . in ways that harm or undermine" the beneficiary.[220] Accordingly, all fiduciaries, at least as Balkin labels them, are "*information fiduciaries*."[221] An information fiduciary is "a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship."[222] Moreover, people and organizations possessing fiduciary duties arising from the use or exchange of information are fiduciaries regardless of whether they do something on the beneficiary's behalf.[223] The information fiduciary model provides a broad cornerstone by which legislators may shape the coverage scope of twenty-first century consumer privacy law in the United States.

211. *Id.* at 1207.
212. *Id.*
213. *Id.*
214. *Id.*
215. *Id.*
216. *Id.* at 1207–08.
217. *Id.*
218. *Id.* at 1208.
219. *Id.*
220. *Id.*
221. *Id.*
222. *Id.* at 1209.
223. *Id.*

2. Data's Fiduciary Rule

The modern digital age has "given rise to new fiduciary relationships created by the explosion of the collection and use of personal data"[224] because there now exists relationships of trust between end-users and online consumer service providers. However, from a regulatory perspective, Balkin argues that these relationships should not be identical to traditional professional fiduciary relationships in all respects because they "may not require the same degree of obligation, loyalty, and protection . . . ."[225] But, these are still fiduciary relationships nonetheless. Balkin notes that "in the digital age, because we trust [consumer entities] with sensitive information," these entities take on fiduciary responsibilities.[226]

Balkin argues we should adopt an information fiduciary regulatory model for twenty-first century consumer privacy protection for four main reasons. First, consumers' relationships with many business entities now involve "significant vulnerability" because these businesses have considerable expertise and knowledge with respect to proprietary online services, and consumers generally lack information about the businesses or what they do with collected information.[227] Second, consumers are "in a position of relative dependence with respect to these companies."[228] Businesses provide many different kinds of services consumers need and consumers must hope that the companies will not misuse their information or abuse their confidence in ways that will harm them.[229] Third, many online service providers and consumer businesses "hold themselves out as experts in providing certain kinds of services in exchange for [consumers'] personal information."[230] Fourth, these entities know they hold valuable data that may be used to consumers' disadvantage, and they understand consumers are aware of this.[231] Thus, these businesses "hold themselves out as trustworthy organizations who act consistent with our interests, even though they also hope to turn a profit."[232] In short, "[b]ecause people understand that they are vulnerable to the collection of personal data, and because they also recognize that the methods used by online service providers are beyond their understanding, they seek reassurance that using these

224. *Id.* at 1221.
225. *Id.*
226. *Id.*
227. *Id.* at 1222.
228. *Id.*
229. *Id.*
230. *Id.*
231. *Id.*
232. *Id.*

services is safe."[233] Unfortunately, most of the details of how companies are utilizing consumers' sensitive information is buried within the "fine print of their privacy policies and in the code of the company's information infrastructure."[234] Therefore, "a changing society generates new kinds of fiduciary relations and fiduciary obligations that the law can and should recognize."[235] Balkin suggests the following formulation for a Data Fiduciary Rule:

> People and business entities act as information fiduciaries (1) when these people or entities hold themselves out to the public as privacy-respecting organizations in order to gain the trust of those who use them; (2) when these people or entities give individuals reason to believe that they will not disclose or misuse their personal information; and (3) when the affected individuals reasonably believe that these people or entities will not disclose or misuse their personal information based on existing social norms of reasonable behavior, existing patterns of practice, or other objective factors that reasonably justify their trust.[236]

Importantly, Balkin notes this formulation of a Data Fiduciary Rule "may require information fiduciaries to protect more things than they have explicitly set out in their privacy policies."[237] Though, this is for the better. As the late Justice Antonin Scalia often noted, "[t]he more speech, the better."[238] Likewise, the more privacy the better. A Data Fiduciary Rule would serve a valuable purpose: "when entities hold themselves out as trustworthy, and when they encourage the disclosure of personal information that places end-users in a vulnerable position, entities should be held accountable . . . ."[239] Also, modern information fiduciaries "may be held to reasonable ethical standards of trust and confidentiality" because of the type of business they engage in.[240]

The Data Fiduciary Rule would also affect third parties. "Fundamentally, a higher legal obligation to users would help shift the

233. *Id.*
234. *Id.*
235. *Id.* at 1223.
236. *Id.* at 1223–24.
237. *Id.* at 1224.
238. Matt Vasilogambros et al., *Scalia Defends* Citizens United *Decision, Reflects on Term in Rare TV Appearance*, THE ATLANTIC (July 18, 2012), https://www.theatlantic.com/politics/archive/2012/07/scalia-defends-citizens-united-decision-reflects-on-term-in-rare-tv-appearance/437268/.
239. Balkin, *supra* note 200, at 1224–25.
240. *Id.* at 1225.

default attitude of data collectors from 'collect everything and ask questions later,' as would holding the service provider responsible for enabling privacy invasions by third parties."[241] Both Balkin and the proposed Data Care Act propose that "fiduciaries should be required to contractually obligate any third parties they share data with to uphold the fiduciary duties they owe their users."[242] Invoking a property concept, "fiduciary obligations must run with the data."[243] "Affirmative legal duties to users, like a prohibition on sharing their information except with entities required to uphold the fiduciary's same duties, would vastly limit incentives to share information" in a reckless fashion.[244]

This model invokes common sense. An information fiduciary model of privacy regulation bears logical resemblance to fiduciary obligations already recognized in American law.[245] For example, consider a doctor, lawyer, or accountant that sold personal information about their clients to a data broker.[246] If these professionals used personal information to manipulate their client's actions for self-interested ends or to gain a business advantage at the expense of their client, they would likely face liability for violating their professional conduct obligations.[247] In essence, the information fiduciary model of privacy regulation merely suggests we extend similar fiduciary principles to those consumer entities which now possess equally sensitive information as professional service providers. Just as in their interactions with doctors, accountants, and lawyers, many consumers assume a sense of personal trust or special confidentiality in their online interactions. Information fiduciaries are no longer just lawyers, doctors, and accountants. In the digital age, they now include our bankers, ride-sharers, social media platforms, digital communications services, and even schools.

"[A]n information fiduciary framework can strike the necessary balance of competing objectives: it is designed to balance commercial prerogatives with meaningful protections for individuals in the way that U.S. privacy law attempts, yet fails, to do."[248] Applying fiduciary duties to data collectors raises the bar of how digital companies are expected to treat user information.[249] "It would help

241. Barrett, *supra* note 35, at 1099.
242. *Id.*
243. *Id.*
244. *Id.*
245. Balkin, *supra* note 200, at 1205.
246. *Id.*
247. *Id.*
248. Barrett, *supra* note 35, at 1087.
249. *Id.* at 1088.

adjust the objective of U.S. privacy law to more heavily prioritize the rights of the user, while still accounting for the commercial prerogatives of the collector."[250] "Duties of loyalty, care, and confidentiality can also prohibit digital harms such as manipulation, discrimination, and other harms that laws exclusively focused on privacy are ill-equipped to prevent, while still permitting non-harmful commercial activity."[251]

Fiduciary rules provide flexibility with respect to professional prerogatives, but they are not "toothless, and they implicate a moral dimension to the regulation of commercial conduct that other consumer protection regulation does not automatically invoke . . . ."[252] Exploiting user information "should not be required for digital products and services to function, and for most of them it is not."[253] Social networks "need not be inherently manipulative, discriminatory, or privacy-invasive—the same is true for an internet service provider, a rideshare company, a medical device company, or a cloud service."[254] Applying fiduciary duties to data collectors requires distinguishing the "kinds of conduct that are inherent to the service—such as a search engine 'discriminating' by sorting through information and only providing the responsive results—from disloyal conduct designed to benefit the data collector to the detriment of the subject."[255]

An information fiduciary framework also solves asymmetric information problems. As in the pre-2008 mortgage markets, modern consumer markets that are reliant on mass data suffer from asymmetric information problems—consumer entities simply possess information with respect to their data practices that consumers do not. Fiduciary concepts may again provide a solution. Fiduciary law assumes that fiduciaries and their beneficiaries are not on "equal footing" because fiduciaries usually possess special skills or knowledge that their beneficiaries lack.[256] The beneficiaries depend upon the fiduciaries to perform certain tasks for them and are often ill-equipped to monitor the behavior of the fiduciaries or prevent them from abusing their relationship of trust, absent any obligations that fiduciary law would supply.[257] Because of information, skill, and knowledge asymmetries, the beneficiaries must trust the

250. *Id.*
251. *Id.*
252. *Id.* at 1091–92.
253. *Id.* at 1092.
254. *Id.*
255. *Id.* at 1089.
256. Balkin, *supra* note 200, at 1216.
257. *Id.*

fiduciaries to act in their best interest.[258] "There are strong asymmetries of information between companies and end users."[259] Company "operations, algorithms, and collection practices are mostly kept secret," most often for sound business reasons.[260] Still, "end-users are not in a very good position to assess how well companies will protect their interests or to decide which company will treat them best in the long run" because "end-users are largely dependent on the good will of these companies not to abuse their personal information."[261] Consequently, these businesses "present the familiar problems that generally give rise to fiduciary obligations."[262] It is difficult for consumers to verify company "representations about data collection, security, use, and dissemination"[263] or to comprehend what companies do with their data.[264] Even if consumers understood these practices, it would be nearly impossible for consumers to monitor them.[265] This situation is analogous to that of financial advisors. Consumers expect that financial advisors will make money from consumers seeking financial advice.[266] However, the fact that consumers expected financial advisors to make money did not prevent the government from attempting to impose fiduciary obligations upon them.[267]

3. Obstacles to Data's Fiduciary Rule, Skepticism, and Supplemental Regulation

Privacy regulations would not be immune to constitutional scrutiny.[268] However, the type of regulation would matter, as privacy regulations concerning the collection and use of data rather than data analysis, disclosure, or sale are less likely to face First Amendment challenges.[269] But, even First Amendment arguments would not doom privacy regulations targeted at data analysis, disclosure, or sale, as when data is "collected, collated, used, and sold in bulk" it is a commodity rather than speech.[270] Specifically, the question arises as to how legislators could keep the information fiduciary

258. *Id.*
259. *Id.* at 1226.
260. *Id.*
261. *Id.* at 1226–27.
262. *Id.* at 1227.
263. *Id.*
264. *Id.*
265. *Id.*
266. *Id.* at 1228.
267. *Id.*
268. *Id.* at 1194.
269. *Id.*
270. *Id.* at 1196.

concept from running afoul of the First Amendment and any right to corporate speech. The answer rests in the law. As Balkin recognized, "when the law prevents a fiduciary from disclosing or selling information about a client—or using information to a client's disadvantage—this does not violate the First Amendment, even though the activity would be protected if there were no fiduciary relationship."[271]

Additional regulation is necessary to supplement any Data Fiduciary Rule. A regulatory framework based exclusively on information fiduciaries would not solve all the problems of "overreaching that will inevitably occur in the age of Big Data."[272] Any consumer privacy fiduciary rule cannot operate in a vacuum if it is to operate successfully. A fiduciary approach is not a replacement for "badly needed structural reforms."[273] Supplemental provisions would also aim to "strengthen existing protections, such as more meaningful obligations to enact reasonable security protocols, and stricter requirements to notify users in the case of breach."[274] For example, opt-in rules could be a helpful supplement to an information fiduciary framework. Such rules can also likely withstand judicial scrutiny, as in 2009 the D.C. Circuit upheld new FCC rules imposing opt-in requirements even in light of a First Amendment challenge.[275]

Also, compliance disasters in the early years of the rule could be an issue. Thus, during a legislative phase-in period, to avoid subjection to penalties under Data's Fiduciary Rule, corporations could be permitted to enter into "best interest contracts" with consumers that affirm fiduciary status and incorporate a duty of loyalty, similar to the BICE the Department of Labor developed following the 2008 financial collapse.[276] The framework proposed by this article is not the only approach to enacting a data fiduciary rule in the consumer privacy realm. For example, there is a more broad and flexible approach that would likely be subject to extensive judicial interpretation and administrative discretion. Ariel Dobkin argues that "informational fiduciary duties should be divided into four categories of behavior: manipulation, discrimination, sharing with

271. *Id.* at 1210; *see id.* at 1211–20 (discussing the difference between speech which is in the public discourse and speech which is removed therefrom and the implications for regulation thereof).

272. *Id.* at 1187.

273. Barrett, *supra* note 35, at 1107.

274. *Id.* at 1097.

275. Balkin, *supra* note 200, at 1203 (citing Nat'l Cable & Telecomms. Ass'n v. FCC, 567 F.3d 659 (D.C. Cir. 2009)).

276. Chamber of Com. v. U.S. Dep't of Lab., 885 F.3d 360, 367 (5th Cir. 2018).

third parties without consent, and violations of a company's privacy policy."[277] "A duty is violated when the fiduciary exceeds a reasonable user's expectations, which those types of conduct will generally do."[278]

But, political conservatives and skeptics need not fear this regulatory framework as being a government overreach, as such a rule would "not apply to everyone. Merely communicating with someone over the Internet does not make [an entity] an information fiduciary."[279] Thus, many business practices concerning consumer data will remain free from regulation.[280] Moreover, the duties legislators may impose on these businesses are likely to be "considerably narrower" than traditional professional fiduciary responsibilities.[281] Also, imposition of fiduciary responsibilities does not mean that all American consumer businesses will suddenly become non-profit entities.[282] The regulatory relationship need not be parasitic or economically harmful; rather, it can be cooperative. "[E]ven though virtual environments are privately owned, governments could create framework statutes that would require platform owners to respect the free speech and privacy rights of end users in return for special legal status and benefits."[283] Ultimately, the legislative process and administrative rulemaking procedures will fashion the precise contours of data's fiduciary rule. Yet, that is beyond the scope of this article.

B. Creation of the Consumer Data Protection Bureau

In the wake of recent data breaches, some have called for the creation of a governmental data protection agency in the United States.[284] Electronic Privacy Information Center (EPIC) suggested that "immediate action" be taken to "address the broader problem of . . . mishandling of consumers' personal data."[285] Reforms should aim to "put consumers back in control of both their credit reports and their personal information."[286] Successful privacy legislation must rely on an enforcement agency that would be given adequate rulemaking authority, civil penalty authority, and sufficient

277. Barrett, *supra* note 35, at 1094.
278. *Id.*
279. Balkin, *supra* note 200, at 1225.
280. *Id.*
281. *Id.*
282. *Id.* at 1227.
283. *Id.* at 1230.
284. *Equifax Data Breach*, *supra* note 56.
285. *Id.*
286. *Id.*

resources and manpower.[287] EPIC notes that with respect to consumer-facing financial institutions, although Dodd-Frank transferred authority over certain privacy provisions to the CFPB, the law did not transfer regulatory authority to establish data security guidelines.[288]

However, the FTC, the federal government's current privacy enforcement arm, is already cooperating with the CFPB.[289] In December 2019, the FTC and CFPB hosted a public workshop to discuss issues affecting the accuracy of traditional credit reports as well as employment and tenant background screening reports. Consequently, the United States should also establish a data protection agency like "virtually every other advanced economy facing the challenges of the digital age."[290] This action is necessary because "[t]he current agencies in the United States tasked with protecting consumers and citizens lack the authority and even the personnel to do what needs to be done."[291]

As to the specific structure and responsibilities of a data protection agency in the United States, one may look to the CFPB for guidance. Accordingly, a Consumer Data Protection Bureau (CDPB) would ideally function as follows. Congress should vest in the CDPB the consumer privacy protection functions of agencies like the FTC, giving the CDPB broad authority in three primary areas—rulemaking, supervision, and enforcement. The CDPB would operate as an independent bureau within the Department of Commerce, not subject to the whim of Congressional appropriations. It would be led by a single director appointed by the President and confirmed by the United States Senate. The CDPB would need adequate manpower to be effective. This enforcement force would likely need to be as large as the CFPB's 1,500 employees,[292] if not larger. The CDPB's authority would be over "covered entities" that, because of their relationship with a consumer, have taken on special duties with respect to the sensitive information they obtain in the course of this relationship.

With respect to rulemaking, the CDPB would have the power to create rules to administer, enforce, and implement federal consumer privacy protection law. Concerning its supervisory

287. Barrett, *supra* note 35, at 1110.
288. *Equifax Data Breach*, *supra* note 56.
289. Press Release, Fed. Trade Comm'n, FTC and CFPB to Host December Workshop on Accuracy in Consumer Reporting (Sept. 19, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/ftc-cfpb-host-december-workshop-accuracy-consumer-reporting.
290. *Equifax Data Breach*, *supra* note 56.
291. *Id.*
292. Lampe & Richardson, *supra* note 123, at 94.

authority, the CDPB would have the power to ensure compliance with the laws and regulations it administers by being able to require reports and examinations of entities to assess their compliance and practices with respect to consumer privacy. To protect start-ups and small businesses, the CDPB's authority could be jurisdictionally-limited to only those entities which meet a certain economic threshold, as Congress would define, focusing upon major companies whose practices implicate consumer privacy—think Google, Facebook, and Equifax. Lastly, an effective CDPB would possess significant authority in the realm of enforcement tools: (1) the power to conduct investigations; (2) the ability to bring public legal actions in federal court or an administrative forum; and (3) the ability to seek injunctive and monetary relief for violations of consumer privacy law by covered entities. Obviously, the CDPB would not be a panacea to all consumer privacy issues. However, it would be a substantial start to bringing the law into alignment with the realities of twenty-first century American life.

C. Data's "Volcker Rule"

Comprehensive consumer privacy legislation in the United States should also include its own version of the Volcker Rule to safeguard consumer data against risky corporate practices. Just as Dodd-Frank's Volcker Rule limited the extent which banks could make risky investments with its depositors' money, a Data Volcker Rule would limit the extent to which businesses could engage in risky practices with consumer data.[293] Third-party data sharing is one possible practice to monitor. Furthermore, the concept of a Data Volcker Rule is not entirely unprecedented. Consider the European Union's General Data Protection Regulation (GDPR). Under the GDPR, institutions that share personal data with third-parties either for storage or processing must ensure the third-party's compliance with the provisions of the GDPR.[294] In the United States, Apple CEO Tim Cook has called for government regulation that would advance two goals: first, increasing the difficulty of data collection by corporate entities; and, second, urging a crackdown on data brokers who transfer consumer data between companies.[295] In sum, comprehensive consumer privacy legislation should guard against "gambling" with consumers' most sensitive information.

293. Ascertaining which specific technological practices are riskier than others with respect to consumer information is beyond the scope of this article; its purpose is to provide a suggestive legislative framework for American consumer privacy law.

294. Stites, *supra* note 53, at 138.

295. Eadicicco, *supra* note 6.

CONCLUSION

Overall, American consumers face a privacy crisis in 2020. The origins of the privacy crisis share numerous parallels to the financial collapse that crippled the American and global economies in 2008. Just as Congress responded to the 2008 financial collapse with comprehensive financial services reform legislation in the form of the Dodd-Frank Act, Congress must respond to the 2020 consumer privacy crisis with comprehensive privacy reform legislation. Congress would be wise to mirror aspects of Dodd-Frank if privacy reform efforts are to succeed, such as including fiduciary obligations, the creation of a new consumer protection agency, and enabling the promulgation of rules designed to limit risky corporate practices. No single piece of legislation will be able to entirely guard against the privacy perils of twenty-first century life, just as no single piece of legislation can entirely prevent economic collapse. Consumers did not lose their privacy in a day; Congress cannot reclaim it instantaneously. However, failing to address the privacy crisis would be an even larger blunder than allowing it to develop in the first place. A Dodd-Frank approach to consumer privacy legislation is a worthy start.